PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-160117
(43)Date of publication of application : 12.06.2001

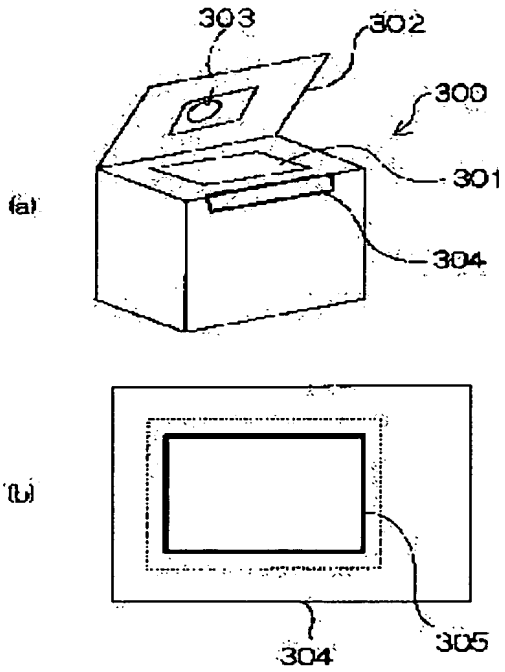
(51)Int.Cl. G06K 17/00
G03G 21/04
G06F 12/14
G06K 19/07
G06K 19/10
H01Q 1/12
H04B 5/02
H04L 9/32

(21)Application number : 11-345330
(22)Date of filing : 03.12.1999

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : ODA YASUNORI

(54) SYSTEM FOR MANAGING DEVICE SECURITY

(57)Abstract:
PROBLEM TO BE SOLVED: To enable a scrupulous control about the operation of a device needing security management such as copying a confidential document.
SOLUTION: A user is made to carry a RFID and a RFID is also attached to the confidential document. A copying machine 300 is provided with a reader/ writer 303 to read the FRID of the document set in the platen and the FRID of the user in front of the machine 300. The machine 300 is controlled so as to be able to copy the document only when the access right of the user read from the FRID of the user is higher than the confidential level of the document read the FRID of the document on the platen.



LEGAL STATUS

[Date of request for examination] 20.05.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2001－160117
(P2001－160117A)
(43)公開日　平成13年６月12日(2001.6.12)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｆ	２Ｈ０２７
			Ｌ	２Ｈ０３４
Ｇ０３Ｇ　21/04		Ｇ０６Ｆ　12/14	３１０Ｋ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３１０		３２０Ｃ	５Ｂ０３５
	３２０	Ｈ０１Ｑ　1/12	Ｚ	５Ｂ０５８

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平11－345330

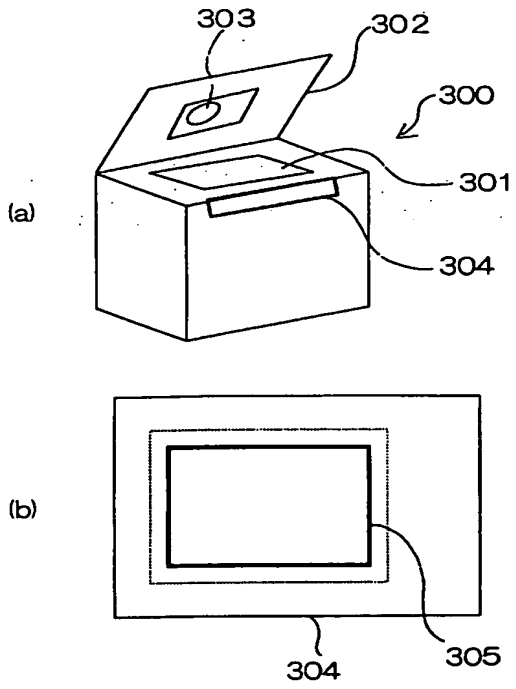
(22)出願日　平成11年12月３日(1999.12.3)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　黄田　保憲
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

最終頁に続く

(54)【発明の名称】　装置セキュリティ管理システム

(57)【要約】
【課題】　機密文書の複写など、セキュリティの管理を要する装置の動作について、きめ細かい制御を可能にする。
【解決手段】　ユーザにＲＦＩＤを携帯させると共に、機密文書にもＲＦＩＤを付ける。複写機３００にリーダ・ライタ３０３を設け、プラテンにセットされた文書のＲＦＩＤと、複写機３００の前にいるユーザのＲＦＩＤとを読み取る。ユーザのＲＦＩＤから読み取った当該ユーザのアクセス権が、プラテン上の文書のＲＦＩＤから読み取った当該文書の機密レベルより高い場合にのみ、複写機３００がその文書の複写を行えるように制御する。



1

【特許請求の範囲】
【請求項１】　対象装置の要セキュリティ動作を管理するシステムであって、
前記対象装置の近傍に設けられ、ＲＦＩＤと通信を行ってそのＲＦＩＤが保持しているセキュリティ情報を取得するＲＦＩＤ通信手段と、
前記ＲＦＩＤ通信手段で２以上のＲＦＩＤから実質的同時に取得したセキュリティ情報が、前記対象装置の前記要セキュリティ動作についての予め登録された許可条件を満足するか否かを判定する判定手段と、
前記判定手段で前記許可条件が満足されたと判断した場合にのみ、前記対象装置に対して前記要セキュリティ動作の実行を許可する動作制御手段と、
を備える装置セキュリティ管理システム。
【請求項２】　前記許可条件は、前記要セキュリティ動作の対象物のセキュリティレベルとその動作を指示するユーザのセキュリティレベルとの関係が如何なる場合に前記要セキュリティ動作の実行を許可するかを示す条件であり、
前記判定手段は、前記対象装置にセットされた対象物に付加されたＲＦＩＤから取得したセキュリティ情報と、ユーザが携帯するＲＦＩＤから取得したセキュリティ情報とから、各々のセキュリティレベルを求め、それらセキュリティレベルの関係が前記許可条件を満足するか否かを判定することを特徴とする請求項１記載の装置セキュリティ管理システム。
【請求項３】　前記許可条件は、前記要セキュリティ動作の各対象物ごとに、その対象物の識別情報とその対象物に対する前記動作を許可するユーザの識別情報との対応を示した情報であり、
前記判定手段は、前記対象装置にセットされた対象物に付加されたＲＦＩＤから取得したセキュリティ情報と、ユーザが携帯するＲＦＩＤから取得したセキュリティ情報とからそれぞれ識別情報を求め、それら識別情報が前記許可条件を満足するか否かを判定することを特徴とする請求項１記載の装置セキュリティ管理システム。
【請求項４】　前記対象装置は複写機であり、
前記判定手段は、前記複写機にセットされた原稿に付加されているＲＦＩＤから取得したセキュリティ情報と、ユーザのＲＦＩＤから取得したセキュリティ情報との組合せが、前記許可条件を満足するか否かを判定することを特徴とする請求項１記載の装置セキュリティ管理システム。
【請求項５】　前記ＲＦＩＤ通信手段のアンテナが、前記複写機の原稿フィーダの原稿受け皿に取り付けられるとともに、この受け皿にユーザのＲＦＩＤをセットするためのくぼみを設け、前記アンテナにより前記受け皿上の原稿に付加されたＲＦＩＤと、前記くぼみにセットされたユーザのＲＦＩＤとに通信を行うことを特徴とする請求項４記載の装置セキュリティ管理システム。

2

【請求項６】　前記ＲＦＩＤ通信手段は、原稿が複写機にセットされた時に、その原稿に付加されたＲＦＩＤとユーザが携帯した当該ユーザのＲＦＩＤとを同時に読み取ることのできるように、前記原稿のＲＦＩＤを含む平面と前記ユーザのＲＦＩＤを含む平面から構成される角度の間になるよう設置された通信用のアンテナを有することを特徴とする請求項４記載の装置セキュリティ管理システム。
【請求項７】　前記ＲＦＩＤ通信手段は、複写機にセットされた原稿に付加されたＲＦＩＤを読み取るための第一のリーダ手段と、
ユーザのＲＦＩＤを読み取ることのできる位置に設置された第二のリーダ手段と、
を有することを特徴とする請求項４記載の装置セキュリティ管理システム。
【請求項８】　前記許可条件は、前記ＲＦＩＤ通信手段で同時に通信したＲＦＩＤの数と、それら各々のＲＦＩＤのセキュリティレベルとの関係から、前記要セキュリティ動作を許可する場合を規定した条件であり、
前記判定手段は、前記ＲＦＩＤ通信手段で同時に取得した１以上のＲＦＩＤの情報が、前記許可条件を満足するか否かを判定することを特徴とする請求項１記載の装置セキュリティ管理システム。
【請求項９】　前記ＲＦＩＤ通信手段は、
セキュリティレベルがコピー可能なことを示すプロパティ情報を含んだ特定ＲＦＩＤを、セキュリティレベルの情報を含んだ所定数の通常のＲＦＩＤと同時に読み取った場合、前記特定ＲＦＩＤに対して前記通常のＲＦＩＤのセキュリティレベルを付与することを特徴とする請求項１記載の装置セキュリティ管理システム。
【請求項１０】　前記判定手段の判定で前記許可条件が満足されなかった場合に、その旨をユーザに通知する通知手段を有することを特徴とする請求項１記載の装置セキュリティ管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】機密文書の複写など、セキュリティを要する装置の動作を制御するためのシステムに関する。
【０００２】
【従来の技術】機密文書は通常、文書上に「機密」または「複写厳禁」などのスタンプを押すなどすることでそれが明示されており、ユーザはその表示を見てその文書の複写などについて相応の注意を払っている。
【０００３】また、各ユーザに課金のために複写枚数を数えるカウンタを持たせ、そのカウンタを複写機にセットしないと複写機が作動しないシステムがある。このシステムは、カウンタを持っている部内者しか複写ができないという意味ではセキュリティの効果をもたらしている。

【０００４】また、人的資源に頼った方式として、機密文書の保管してある部屋をガードマンやそれに類する人によって管理することがよく行われている。また、複写担当者を介してしか文書複写をできないような運用を行っている場合もある。

【０００５】また近年では、機密文書を、紫外線や赤外線などの非可視光の下でしか読めないような特殊なインクを使って印刷することも行われている。この場合、専用光源のある閲覧室では機密文書を読むことができるが、その機密文書を一般の複写機で複写しようと思っても、一般の複写機は可視光線の反射波を利用するので、可視光線を反射しにくいインクを使った機密文書は複写できない。

【０００６】しかしながら、全く何もできなることによる不便さや、その特殊な文書を作る煩わしさが汎用の妨げとなっている。

【０００７】

【発明が解決しようとする課題】「機密」等の表示を行う方式は、ユーザのモラルに頼った方式であり、セキュリティ面から見て十分とは言えない場合が多い。

【０００８】各ユーザに複写カウンタを持たせる方式は、カウンタさえ持っていればどのような文書でも複写できるので、機密文書の複写管理という観点からは十分なセキュリティが確保できているとは言い難い。

【０００９】ガードマン等により管理を行う方式は、コスト面で問題が多く、また結局は人間のモラルに頼っているといえる。

【００１０】また、機密文書に特殊インクを用いる方式は、不正複写防止という観点から見れば高いセキュリティが得られるが、正当なユーザが不便を強いられるという問題がある。すなわち、特殊インクを使った場合、機密文書を読むのにも特殊な光源を要し、また機密文書を印刷するのにも特殊な複写機を要する。

【００１１】このように従来の機密文書の複写の管理方式は、いずれも問題があった。以上、機密文書の複写の場合を例にとったが、ユーザに対して提供するサービスにセキュリティの管理を要する状況は多々あり、そのようなセキュリティ管理を自動化した例も、例えば機密区画の入退室管理装置などのように多い。このようなセキュリティに係る装置の動作管理は、例えばユーザにＩＣカードを持たせ、このカードを装置に挿入するなどの方式で行われているが、それだけでは不十分な場合や、不便な場合もある。例えば複写の場合で言えば、文書の機密の程度によってどのレベルのユーザまで複写を許すかなどの、きめ細かい管理を行うには、ＩＣカード等でユーザ確認を行うだけでは不十分でである。また、例えば、入退室管理装置では、ビジター（一時的な訪問者）の出入りのために有効なカードを持つホスト側の人間が付き添っていなければならないなどの不便がある。

【００１２】本発明はこのような問題に鑑みなされたものであり、セキュリティを要する装置の動作をきめ細かく制御するための仕組みを提供することを目的とする。

【００１３】

【課題を解決するための手段】上記目的を達成するため、本発明に係る装置セキュリティ管理システムは、対象装置の要セキュリティ動作を管理するシステムであって、前記対象装置の近傍に設けられ、ＲＦＩＤと通信を行ってそのＲＦＩＤが保持しているセキュリティ情報を取得するＲＦＩＤ通信手段と、前記ＲＦＩＤ通信手段で２以上のＲＦＩＤから実質的同時に取得したセキュリティ情報が、前記対象装置の前記要セキュリティ動作についての予め登録された許可条件を満足するか否かを判定する判定手段と、前記判定手段で前記許可条件が満足されたと判断した場合にのみ、前記対象装置に対して前記要セキュリティ動作の実行を許可する。

【００１４】このシステムによれば、対象装置に関わる複数のＲＦＩＤの情報に基づきその装置の動作が制御できるので、きめ細かなセキュリティ管理が可能になる。

【００１５】本発明の好適な態様では、前記許可条件は、前記要セキュリティ動作の対象物のセキュリティレベルとその動作を指示するユーザのセキュリティレベルとの関係が如何なる場合に前記要セキュリティ動作の実行を許可するかを示す条件であり、前記判定手段は、前記対象装置にセットされた対象物に付加されたＲＦＩＤから取得したセキュリティ情報と、ユーザが携帯するＲＦＩＤから取得したセキュリティ情報とから、各々のセキュリティレベルを求め、それらセキュリティレベルの関係が前記許可条件を満足するか否かを判定する。

【００１６】この態様では、要セキュリティ動作の対象物のＲＦＩＤと、ユーザのＲＦＩＤから各々のセキュリティレベルを取得し、それら両者の関係に基づきその動作の実行が許可できるかを判定する。例えば複写機を例にとった場合、複写機が対象装置に対応し、機密文書の複写動作が要セキュリティ動作に、機密文書がその対象物に、それぞれ対応する。この態様によれば、対象物とユーザの関係に基づき、要セキュリティ動作の実行を詳細に管理できる。

【００１７】別の好適な態様では、前記許可条件は、前記ＲＦＩＤ通信手段で同時に通信したＲＦＩＤの数と、それら各々のＲＦＩＤのセキュリティレベルとの関係から、前記要セキュリティ動作を許可する場合を規定した条件であり、前記判定手段は、前記ＲＦＩＤ通信手段で同時に取得した１以上のＲＦＩＤの情報が、前記許可条件を満足するか否かを判定する。

【００１８】この態様では、例えば複数人で相互の信用保証が期待される場合などにも一定の要セキュリティ動作の実行が可能になり、一人の認証情報に基づき要セキュリティ動作を行っていた従来的な管理方式に比べて、現場のニーズに合わせたきめ細かな動作許可の条件設定が可能になる。

【００１９】また別の好適な態様では、前記ＲＦＩＤ通信手段は、セキュリティレベルがコピー可能なことを示すプロパティ情報を含んだ特定ＲＦＩＤを、セキュリティレベルの情報を含んだ所定数の通常のＲＦＩＤと同時に読み取った場合、前記特定ＲＦＩＤに対して前記通常のＲＦＩＤのセキュリティレベルを付与する。

【００２０】この態様では、特定ＲＦＩＤと所定数の通常のＲＦＩＤとをほぼ同時にＲＦＩＤ通信手段の通信範囲内に入れるだけで、通常のＲＦＩＤのセキュリティ情報をその特定ＲＦＩＤにコピーできるので、入退室管理システムなどにおいて、訪問者やＩＤカードを忘れた者等に対して発行する仮カードに対してその者が必要とするセキュリティ許可内容を書き込むのが容易になる。

【００２１】

【発明の実施の形態】［実施形態１］本実施形態では、複写機による機密文書の複写管理を例にとる。したがってこの実施形態では、複写機が特許請求の範囲の「対象装置」に該当する。ここでは説明を簡単にするため、セキュリティ管理のための情報処理装置および記憶装置は、複写機とは別体のパーソナルコンピュータをベースに構築されているとする。ただし、最近の複写機は、内部に高性能のＭＰＵや大容量の記憶装置を有している場合が多く、以下に説明するセキュリティ管理の情報処理機能を複写機に組み込むことは容易である。

【００２２】本実施形態では、セキュリティ管理のためにＲＦＩＤ（Radio Frequency Identification）を用いる。ＲＦＩＤは、非接触読取型のデータキャリアであり、記憶用のＩＣチップと通信用のアンテナとを内蔵する。ＲＦＩＤは、プラスティックカード形式のものが一般的であるが、可撓性をもつ薄いタグの形のものも開発されている。記憶容量の小さいＲＦＩＤはトランスポンダーと呼ばれることもある。ＲＦＩＤはその通信方式（利用する通信周波数等）によって、主に４種類のものに分類される。この分類は、ＲＦＩＤとそれに読み書きを行うリーダ・ライタとの通信距離に応じて名付けられており、通信距離が短い順に、密着型、近接型、近傍型、マイクロ波型と呼ばれている。密着型は短波の静電誘導を利用したもので、その通信距離は数ミリである。近接型は短波の電磁誘導を利用したもので、その通信距離は1cmから30cmくらいである。近傍型は長波の電磁誘導を利用したもので、その通信距離は30cmから70cmくらいである。マイクロ波型は文字どおりマイクロ波の電磁誘導を利用したもので、通信距離は3mから10mくらいである。マイクロ波型のＩＣカードは電源として電池を利用する場合が多いが、他の３つの型のカードはリーダ・ライタからの電磁誘導等により電源を得る無電池のものが普通である。本実施形態では、近傍型乃至マイクロ波型の使用を想定する。

【００２３】図１に示すように、本実施形態のシステムは、一つの機密室１００内に構築される。複写管理の対象となる機密文書は書棚１０８に保管されている。図２に示すように、機密文書２００には、ＲＦＩＤ２０１が貼付されている。書棚１０８と複写機１０６は同じ機密室１００内にあり、その入り口はリーダ・ライタ１０３のついたドア１０７で守られている。

【００２４】リーダ・ライタは、ドア１０７の部分だけでなく、複写機１０６と書棚１０８にも設けられている（リーダ・ライタ１０２及びリーダ・ライタ１０９）。各リーダ・ライタ１０２，１０３，１０９は、セキュリティ管理装置１０４に接続されている。セキュリティ管理装置１０４には、各ユーザや各文書のＩＤ番号や後述する機密文書の複写許可の条件などを記憶した記憶装置１０５が接続されている。各リーダ・ライタは、例えば一定間隔（例えば数十ミリ秒から数秒程度）ごとに、あるいは特定のイベントが発生したときに、質問波を発する。リーダ・ライタの通信可能な範囲内にＲＦＩＤがあれば、そのＲＦＩＤは自己の保持するデータで変調した応答波を返信する。各リーダ・ライタは、この応答波を受信すると、その応答波に含まれるデータを抽出し、セキュリティ管理装置１０４に送信する。

【００２５】図２に示すように、各ユーザ２０２は、ＲＦＩＤ２０３を携帯するものとする。もし、ＲＦＩＤ２０３を携帯しないユーザが機密文書を持ち出そうと思っても、リーダ・ライタ１０３で有効なＲＦＩＤ２０３を検知しない限りセキュリティ管理装置１０４はドア１０７の開動作を許可しないので、そのユーザは機密室１００内に入れない。また有効なＲＦＩＤを携帯するユーザでも、機密文書のセキュリティレベルを満足しない者が機密文書を機密室１００から持ち出そうとすると、セキュリティ管理装置１０４はドア１０７を開かないようにする。もちろん、入室する場合にも携帯するＲＦＩＤのセキュリティレベルをチェックしてドアの開閉を行うようにする。

【００２６】なお、リーダ・ライタは通常、ＲＦＩＤと電波で通信するアンテナと、このアンテナで送信する質問波や受信する応答波を処理したり、セキュリティ管理装置１０４とデータのやり取りを行う制御部から成り立っている。以下では、詳細が必要でない場合は、リーダ・ライタのアンテナ、制御部などと区別して書くことはせず、単にリーダ・ライタと書くことにする。

【００２７】複写機１０６に取り付けられたリーダ・ライタ１０２は、複写のためにセットされた機密文書のＲＦＩＤ２０１とユーザのＲＦＩＤ２０３を実質的に同時に読み込めるように配設されている。

【００２８】リーダ・ライタ１０２のアンテナは、図３（ａ）に示すように、複写機３００において、複写される原稿を押さえるカバー３０２に埋め込まれている。図３（ｂ）は、複写機３００のカバー３０４の押さえ側の面にリーダ・ライタの別の形（矩形）のアンテナ３０５を設けた例を示す。ユーザは、原稿を複写面３０１上に

置いてこのカバー３０２を閉めたのち、そのカバー３０２上に、自分のＲＦＩＤ２０３を置く。すると、リーダ・ライタ１０２は、複写面上の原稿に取り付けられたＲＦＩＤと、カバー３０２上のユーザＲＦＩＤと通信（質問波と応答波のやり取り）を行い、各々の保持するセキュリティ情報を取得し、管理装置１０４に送る。なお、セキュリティ管理装置１０４は、ユーザのＲＦＩＤが検知されない（すなわちユーザＲＦＩＤのセキュリティ情報がリーダ・ライタ１０２に届かない）時には、複写機１０６に対して複写を許可しない。すなわち、機密室１００内の複写機１０６は、基本的にセキュリティ管理装置１０４から動作許可を受けない限り、複写動作を実行できないように構成されている。

【００２９】機密文書のＲＦＩＤとユーザのＲＦＩＤが保持するセキュリティ情報のデータ構造は、例えば図４に示すようなものである。すなわちセキュリティ情報は、ＲＦＩＤの固有のＩＤ番号４０１とセキュリティレベル４０２から成り立っている。ＩＤ番号４０１が、そのＲＦＩＤが貼付された文書、あるいはそのＲＦＩＤを携帯するユーザの識別情報となる。セキュリティ情報は、これ以外にも各種のデータを含みうるが、本実施形態に関わるのはこの２つのデータなので、ここではそれらを挙げるにとどめる。

【００３０】セキュリティレベル４０２は、文書の場合は例えばその文書の機密の度合いを表す正の整数であり、例えばその数値が大きいほど機密度が高い。一方、ユーザのＲＦＩＤのセキュリティレベル４０２は、ユーザが取扱を許されている最高の機密度を表す数値である。したがって、ユーザのＲＦＩＤのセキュリティレベルが、文書のＲＦＩＤのセキュリティレベル以上でない場合、ユーザはその文書を持ち出したり、複写したりできないように管理される。すなわち、機密文書のセキュリティレベルがＫで、ユーザのセキュリティレベルがＭの場合、Ｍ≧Ｋの時に限って複写機が動作するようにする。

【００３１】ＲＦＩＤを用いた複写管理のプロセスを図５に示す。図５のフローチャートは、管理装置１０４の処理動作を示している。ユーザが、複写機１０６のスタートのボタンを押すと、このイベントが複写機１０６のコントローラから管理装置１０４にその旨が伝わる。これを受けた管理装置１０４は、複写機１０６のリーダ・ライタ１０２に対して、質問波発射の命令を送る（ステップ１００１）。この命令を受けたリーダ・ライタ１０２はアンテナから質問波を送り、これに対する複写面３０１に置かれた機密文書のＲＦＩＤとカバー３０２の上に置かれたユーザのＲＦＩＤからの応答波を受け取る（ステップ１００２）。応答波が無ければ（すなわちリーダ・ライタ１０２から、ＲＦＩＤのセキュリティ情報が伝送されてこなければ）、ステップ１００２の判定結果が否定（Ｎ）となり、この場合管理装置１０４はなにもせずに処理を終了する。従ってこの場合複写機１０６には複写動作の許可が与えられないので、複写機１０６は複写は行わず、待機状態となる。応答波があれば、管理装置１０４は、その応答波のセキュリティ情報から文書及びユーザのセキュリティレベルをそれぞれ求め、両者を比較する（ステップ１００３）。もしユーザのセキュリティレベルが文書のセキュリティレベル未満であれば、ステップ１００３の判定結果が否定（Ｎ）となる。この場合は、管理装置１０４は何も行わずに処理を終了する。すなわちこの場合、管理装置１０４から複写機１０６に複写動作許可の信号が送られないので、複写機１０６は複写動作禁止のまま待機する。ステップ１００３の判定で、ユーザのセキュリティレベルが文書のセキュリティレベル以上であれば、ステップ１００４にに移り、管理装置１０４は複写機１０６に対して複写動作許可命令を送る。これにより、複写機１０６は複写動作が可能な状態となり、複写面３０１上の文書の複写を行う。複写が終われば、管理装置１０４は、再び、複写機１０６からスタートボタン押下イベントを報せる通知を待つ状態となる。

【００３２】以上のような処理により、機密文書の機密度と、ユーザに与えられた機密アクセス権との両方を考慮した、きめ細かい複写管理を行うことができる。

【００３３】また、本実施形態のシステムでは、以上のようなセキュリティレベルを利用した複写管理の他に、文書毎に特定のユーザに限って複写を許すような管理も可能である。この場合、管理装置１０４に、許可条件を表す図６に示すようなテーブルを設ける。図６には３種類のテーブルの例を示している。テーブル（ａ）では、各機密文書ごとに、そのＩＤと、その機密文書の取扱（複写や持出）を許可するユーザのＩＤとが登録されている。このテーブルを用いて管理を行う場合、管理装置１０４は、複写機１０６のリーダ・ライタ１０２から送られてきた文書及びユーザのＲＦＩＤのセキュリティ情報から、文書及びユーザのＩＤ番号をそれぞれ抽出し、このテーブルを参照してそのユーザがその文書の複写を許可されているかどうかを判定する。したがって、この方式の場合は、ＲＦＩＤにはＩＤ番号の情報のみが含まれていればよく、セキュリティレベルの情報は必要ない（図４の例と比較）。

【００３４】図６の（ｂ）のテーブルは、文書のセキュリティレベルごとに、そのレベルの文書に対する取扱を許すユーザのＩＤが登録されている。この場合、管理装置１０４は、リーダ・ライタ１０２から受け取った文書のセキュリティレベルの情報とユーザのＩＤ番号の情報から、このテーブルを参照してそのユーザがその文書の複写を許可されているかどうかを判定する。

【００３５】図６の（ｃ）のテーブルは、各文書ごとに、そのＩＤと、その文書に対する取扱を許すユーザのセキュリティレベルの条件が登録されている。この場

合、管理装置１０４は、リーダ・ライタ１０２から受け取った文書のＩＤ番号とユーザのセキュリティレベルから、そのユーザがそのテーブルに示されている条件を満足しているかどうかを判定する。

【００３６】管理装置１０４は、このようなテーブルに基づく判定の結果、複写の許可条件を満足していれば、複写動作許可信号を複写機１０６のコントローラに送る。そうでなければ、管理装置１０４は何もせず、その結果複写機１０６は動かないままとなる。

【００３７】一つの方式としては、複写が一回行われる度に、複写機１０６のコントローラは、デフォルトの複写動作不可状態とする。そして、ユーザが複写スタートのボタンを押す度に、文書に付加されたＲＦＩＤとユーザのＲＦＩＤとが読み直されるようにする。なお、これはあくまで一例である。

【００３８】なお、機密文書を保管する書棚１０８に扉とリーダ・ライタ１０９を設け、セキュリティ管理装置１０４でその扉の開閉等を制御することで、より高度の機密を保てる。すなわち、リーダ・ライタ１０９で書棚１０８の近傍に来たユーザのＲＦＩＤのＩＤ番号を識別するようにし、ＩＤ番号が検知できなかった場合には扉が開かないようにするなどである。この方式では、書棚１０８を開けたユーザのＩＤを管理装置１０４で記録することもできる。また更には、書棚１０８からユーザが取り出そうとした文書のＲＦＩＤをリーダ・ライタ１０９で読み取り、複写管理の場合と同様、その文書とそれを取り出そうとしたユーザのセキュリティレベルを検査し、そのユーザがアクセスを許可されていない文書であることが判明した場合には、管理装置１０４からしかるべき管理者に警報を発するなどの処置がとれる。

【００３９】このように、本実施形態では、機密文書の複写に関して、ユーザ及び文書の両面からきめ細かい機密管理を行うことができ、機密事項の不要な漏洩を防ぐことができる。

【００４０】［実施形態２］この実施形態は、複写管理におけるユーザＲＦＩＤの取扱に関するものであり、請求項５に関わる。

【００４１】本実施形態では、図７に示すように、複写機５００（上部構造のみ図示）のリーダ・ライタのアンテナ５０２を、原稿フィーダ５０１の原稿受け皿に装着する。この構成において、リーダ・ライタのアンテナ５０２は、フィーダ下部の原稿スキャン位置の部分をカバーするように取り付ける。ユーザのＲＦＩＤは、フィーダ５０１の受け皿に設けられた窪み５０３に置いてもらう。この上に複写したい文書を置いてもらえば、複写動作に支障を来さずに、ユーザと文書のＲＦＩＤの両方を読み取ることができる。この場合、一枚でも読み込み不可の原稿が生じると複写が出来なくなる。一枚一枚調べて複写可能か調べるには次のようにする。

【００４２】すなわち、別のアンテナ配置として、受け皿上の原稿が複写面（プラテン）まで搬送される際に回転して通るフィーダ５０１のコーナー部５０４をカバーする位置にアンテナを設けることも好適である。この場合ユーザのＲＦＩＤは、フィーダ５０１のコーナー部分５０４の上に置いてもらうようにすればよい。この場合も、複写時の原稿搬送を妨害することなく、原稿及びユーザのＲＦＩＤの読み取りを行うことができる。

【００４３】本実施形態のセキュリティ管理処理は、基本的に実施形態１と同様である。ただし、原稿を自動送りする原稿フィーダ５０１を用いるので、セキュリティ管理装置１０４はこの点の配慮した制御を行う。

【００４４】すなわち、複写機の制御状態は複写が一枚行われるごとに複写禁止状態にリセットする。そして、文書をフィードして読み取る際に、その文書のＲＦＩＤを読み取ってそのセキュリティレベルを確認する。ここで、セキュリティレベルのチェックで、そのユーザがその文書を複写できないと判定された場合、例えば、その文書を複写することなく排紙し、次の文書をフィードするようにすることが好適である。この場合、書類の読みとりを中断することなく、複写可能なものだけ複写出来る。

【００４５】この処理の手順は、図５に示した実施形態１の処理手順アルゴリズムにおいて、ステップ１００１の前に『文書を一枚複写面にフィードするという命令を複写機のコントローラに送る』というステップを加え、終了の処理の代わりにループを作り、上記のフィード処理の前にアルゴリズムのコントロールが戻るようにすれば実現できる。原稿をフィードしても何も送られなくなった時点で、アルゴリズムを終了させればよい。

【００４６】この実施形態によれば、複数の文書を、機密管理しつつ、連続的に複写することができる。

【００４７】［実施形態３］この実施形態は、複写機のリーダ・ライタのアンテナ構成の別の形態に関するものであり、請求項６と７に関する。

【００４８】実施形態１及び２では、ユーザは携帯するＲＦＩＤを複写機の上に置かねばならなかった。この例ではユーザがＲＦＩＤを携帯したまま複写が可能なようにアンテナを配置する。

【００４９】第一の方式は、文書を読むリーダ・ライタの他に、ユーザ用の第二のリーダ・ライタを、例えば複写機の手前側に取り付けるというものである。文書用のリーダ・ライタとユーザ用のリーダ・ライタは、通信領域が異なるので同時に電波を送り、読み取りが開始できる。ユーザ用のリーダ・ライタのアンテナは、図３で言えば、複写機の上面と前面の交わる角の部分３０４に設ける。このアンテナとしては、複写機の前に立ったユーザのＲＦＩＤの位置（例えばユーザの胸から腰の辺り）をカバーする程度の通信距離のものを選べばよい。

【００５０】第二の方式では、ループアンテナを複写機の前面に付ける。ループアンテナは通常その前と後ろに

同じ形で通信領域ができるので、一方は複写機上の文書のＲＦＩＤを読むことができ、もう一方の通信領域で、腰につけたユーザのＲＦＩＤを読むことが出来る。なお、複写機は金属でできており、この通信領域は金属によって影響を受けるので通信電力やアンテナの形状や設置場所に充分注意を要する。また、複写に用いるトナーは帯電しているので、トナーが付けられるローラーの部分に電波が行かないように工夫する必要がある。例えば、アンテナの複写機内部側の一部を金属などで遮蔽すればよい。

【００５１】第三の方式は、ループアンテナの一つの通信領域で２つのＲＦＩＤを読みとるというものである（上記第二の方式では、ループアンテナの両側にできる２つの通信領域で２つのＲＦＩＤを読み取った）。この方式では、アンテナの向きを充分に考慮する必要がある。ここで、アンテナの「向き」とはアンテナのデバイスから通信距離が最大になる方向のことを言う。アンテナがループ状の場合、アンテナの向きはループを含む平面に対し垂直の方向になる。もし、アンテナの向きがユーザの携帯するＲＦＩＤ（のアンテナ）に平行であれば、ユーザのＲＦＩＤの小アンテナにアンテナからくる磁束が通りにくくなり、ユーザのＲＦＩＤが読み取りにくくなる（一般に複写面上の文書は水平であり、ユーザが携帯するＲＦＩＤは垂直（首からつり下げるなど）である）。またアンテナの向きを、複写面に平行にすると、文書のＲＦＩＤに対してアンテナの向きが平行になり、今度は同様に文書のＲＦＩＤが読みにくくなる。従って、アンテナをユーザのＲＦＩＤの向きと複写面の向き（これらは互いに直角）の両方に平行にならないように設置すれば、上記のような問題は解消される。例えば、複写面によって規定される水平面と、複写機前面に立ったユーザに向かい合う垂直面と、のそれぞれから４５度の角度になるようにアンテナの向きを設定すれば、ユーザ、文書双方のＲＦＩＤが読めることになる。図示すれば、図８に示すように、リーダ・ライタのアンテナは、ＲＦＩＤ１１０１が取り付けられた文書１１０５がセットされる複写機１１００の複写面によって規定される水平面と、その前（操作パネル側）に立ったユーザ１１０４（ＲＦＩＤ１１０２）に対向する垂直面との間の９０度の角度の範囲１１０３のなかで、できるだけ４５度に近い向きに配設すればよい。

【００５２】この実施形態によれば、一つのリーダ・ライタで、ユーザがＲＦＩＤを複写機上に置くなどの煩雑な動作をすることなく、ユーザのＲＦＩＤと文書のＲＦＩＤと同時に読むことができ、複写機の機密動作制御ができる。

【００５３】［実施形態４］この実施形態は請求項８に関する。

【００５４】通常、入退出管理システムでは、一人のユーザがＲＦＩＤを内蔵するカードを入りロドア付近に設置されたリーダ・ライタにかざすことで、ドアの開動作を要求する。このとき、リーダ・ライタはＲＦＩＤのセキュリティ情報を読み取り、その情報をセキュリティ管理装置（例えば図１の装置１０４）に送る。管理装置は、そのセキュリティ情報の中のＩＤ番号が、その部屋の中へのアクセスが認められた正当なＩＤであるかどうかを、所定の管理データ・ベースを参照して判定し、正当なＩＤであれば、ドアを開け、そうでなければドアを開けない。

【００５５】この方式は、非常に厳格な管理方式であり、場合によっては厳格すぎて不便になることもある。例えば、たまたまカードを忘れた場合、機密室１００に入ることが出来ず、必要な作業ができなくなることも考えられる。このような場合、仮のＩＤカードを発行してそのユーザにもってもらうなどの対処を行うことが多いが、１つの建物内に機密レベルの異なる複数の部屋がある場合も多く、そのような場合仮のＩＤカードでは、当人の本当のＩＤカードと同様のセキュリティクリアランスが得られない場合があって不便になることがある。

【００５６】また、入退室管理装置では、一般に、一人が有効なカードを持っていれば、それに同行した人はカードを持たなくても、カードが持っている人がドアを開けることによって同行者の入室が可能である。ただし、この場合も、有効なカードを持った特定の人（ガードマンなど）が居ないと、その人が来るまで大変な時間を待たされるということがあり、不便である。

【００５７】さて、機密度の高い部屋は、一般に利用する人が限られている。したがって、利用者が２人またはそれ以上いる場合、特別の管理者が居なくても、互いが信用保証をすることができる。すなわち、機密度の高い部屋の利用者は互いを知っていることが多く、お互いの信用を保証できる場合が多い。したがって、複数人の利用者の信用度によって入室を可能にすることにより、セキュリティを保証しながら利便性を達成することになる。本実施形態では、この考え方に従って、セキュリティと利便性をある程度まで両立した入退室管理を行う。

【００５８】なお、このように、２人以上いればセキュリティの保証がなされてある物事がなされる例はいくつもある。 例えば、銀行の旧来方式の貸し金庫なども、本人の鍵と銀行側の鍵があって初めて、該当金庫を開けることができ、これは複数人による信用保証の一種と考えられる。

【００５９】また、危険物あるいは劇薬などの管理室に入るのに、その部屋は特定の人しか利用しないのに、いちいちガードマンに許可をもとめ、ドアを開けるなどの処置がなされる場合がある。これも利用者が数人が居ることで、互いの信用保証を獲得するようにすれば、入室が可能となり利便性が増すとともに、場合によってはガードマンを廃止して人権費を減らすこともできる。病院などでは、癌患者や難病者の苦痛を押さえるためにモル

ヒネを利用することがある。このモルヒネは麻薬とも見られているので院長しかモルヒネを保管している金庫が開けられないことが多い。しかし、夜中や院長が居ない場合に突然モルヒネが必要となる場合がある。例えば、医師二人がいれば、または医師一人と看護婦２人がいれば、金庫を開けても良いなどのルールを決め、そのルールに従って管理が行えれば、緊急の際の利便性が向上するのは言うまでもない。

【００６０】また、上記実施形態１，２，３では、一方のＲＦＩＤは書類に付加されたものであるが、もう一方はユーザの携帯するＲＦＩＤであり、両者がセキュリティレベルが満足されたときのみ複写機を動かすことができた。両者のＲＦＩＤはそれを保持するもの（属性）が違うが、セキュリティのコントロールの面やコントローラの制御のアルゴリズムにおいては、実施形態１，２，３も複数のＲＦＩＤのセキュリティ情報の関係に基づき、管理対象の装置の動作を管理するシステムの一種と捉えることができる。

【００６１】ユーザに付与されるセキュリティレベル（機密アクセス権）にはいくつかの段階がある。どのようなセキュリティレベルの人がどれだけ集まれば信用保証がなされ（入室や金庫扉のオープン、その他の処理が認められ）るかのルールを定めておき、リーダ・ライタで同時に読みとった各人のＲＦＩＤのセキュリティレベルがそのルールを満足するかをセキュリティ管理装置１０４で判定して入室等の処理を管理すれば、きめ細かなセキュリティ管理が可能である。

【００６２】ルールとしては、例えば単純な例としては、一番高いセキュリティレベルでは一人で入室（または処理）が可能になり、二番目のレベルではＫ（＞１）人以上いれば入室が可能になり、それ以下のレベルでは入室が不可であるというようなルールが考えられる。以上は非常に単純な例であったが、医師１人と看護婦２人以上が同時にいれば金庫を開けるのを許す、という場合なども、セキュリティレベルを用いてルール化できることは明らかであろう。本実施形態では、このような複数人のセキュリティレベルの組合せに基づいて、ドア開閉などの所定の処理動作を制御する機構を提供する。

【００６３】本実施形態の処理手順は、図９～図１１のフローチャートに示される。以下では、入室管理における入りロドアの開閉装置の制御を例にとって説明するが、同様のセキュリティ管理が複写機その他セキュリティ管理を要する装置の動作制御に応用可能なことは以下の説明から容易に理解されるであろう。

【００６４】以下、本実施例のアルゴリズムを図９～図１１のフローチャートに基いて説明する。ここでは入室管理を例にとるので、システム構成としては図１を参照されたい。

【００６５】図９に示すように、入りロのリーダ・ライタ１０３は一定間隔で質問波を繰り返し送信し、ＲＦＩＤからの応答波を確認している（ステップ６０１）。応答波が無ければステップ６０１の判定が否定（Ｎ）となり、ループが繰り返される。

【００６６】応答波があった場合、セキュリティ管理装置１０４は、確認できたＲＦＩＤが１つだけか否かの判定をステップ６０２にて行い、ＲＦＩＤが一個しか確認できない場合は、ステップ６０３に移行し、２個以上確認できる場合には、ステップ６０４に移行する。ステップ６０３の手続きの詳細は図１０のフローチャートで記述され、ステップ６０４の手続きの詳細は図１１のフローチャートで示される。

【００６７】図１０を参照してステップ６０３の詳細な手順を説明する。この手順は、リーダ・ライタがＲＦＩＤを一つしか確認しなかった場合である。この場合、セキュリティ管理装置１０４は、ステップ７０１で、確認したＲＦＩＤのセキュリティレベルが、入りロドアの開動作の許可を受けられるレベルかどうかを判断される。

【００６８】もし、許可を受けられるレベルであれば、制御の対象の装置（ここではドアの開閉装置）のコントローラに動作許可の命令を送る（ステップ７０２）。そうで無ければ、対象装置に動作許可を送らず、警告処理等のエラー処理を行う（ステップ７０３）。ステップ７０３の場合、対象装置であるドア開閉装置は動作許可を得ていないので、ドアを開かない。ステップ７０２又は７０３が終わると、ステップ６０１に戻る。

【００６９】図１１を参照して、ステップ６０４の詳細な手続きを説明する。この手順は、ＲＦＩＤが複数枚確認出来る場合の処理である。この場合、管理装置１０４は、ステップ８０１で、同時に確認できた複数のＲＦＩＤのセキュリティレベルが、予め管理装置１０４に登録されている対象装置（ドア開閉装置）の動作許可条件を満たしているかどうかを判定する。図１１の例では、前に例示した単純なルール（あるレベルの人がＫ人以上居ればよい、というルール）の場合を示している。この場合、ステップ８０１にて、所定のセキュリティレベル以上のＲＦＩＤがＫ枚以上あるかを判断する。もしそうであれば（ステップ８０１の結果がＹ）、対象装置であるドア開閉装置のコントローラに動作許可の命令を送る（ステップ８０２）。これにより、入りロのドアが開かれ、人々が室内に入れるようになる。ステップ８０１の判定結果が否定（Ｎ）の場合、警告処理等のエラー処理を行う（ステップ８０３）。この場合、ドア開閉装置は動作許可を得ていないので、ドアは開かない。ステップ８０２又は８０３が終わると、ステップ６０１に戻る。

【００７０】以上は単純な例で説明したが、ステップ８０１の動作許可の判定のためのルールには、様々なバリエーションが考えられる。例えば、「レベル３～５の人が１人以上かつレベル１～２の人が２人以上いれば、許可する」など、各セキュリティレベルごとに必要とする人数を定めるルールも考えられる。また、セキュリティ

レベルの値をポイントと考え、同時に読み取ったＲＦＩＤのセキュリティレベルの総和が、所定のしきい値以上となったら許可する、等のルールも考えられる。

【００７１】このように、本実施形態によれば、複数人のセキュリティレベルの関係から対象装置（例えばドア開閉装置）の動作を制御できるので、１人の人間のセキュリティ情報のみに基づいてセキュリティ管理を行っていた従来システムに比べ、より柔軟なシステムが構築できる。

【００７２】［実施形態５］この実施形態は請求項９に関わる。

【００７３】入退室管理において、ビジター（訪問者）は、一般の場合、有効なＩＤカード（ＲＦＩＤ）を持った関係者が同行することで入室を可能にすることが多い。関係者であっても、ＲＦＩＤのカードを忘れた場合は、ガードマンに入れて貰ったり、守衛所で名前を登録してドアの開閉不可能なバッジ等が支給されたりする。いずれにせよ、ドアのところで誰かに開けて貰わなければならない。特に関係者本人がＩＤカードを忘れた場合、不便であり、生産性が下がる。

【００７４】そこで、本実施形態では、ビジターやＲＦＩＤカードを忘れた関係者に対し、仮のＲＦＩＤを発行し、その仮カードに対して、他の関係者からの認証により、セキュリティレベルを自動付与する機構を提供する。すなわち、本実施形態では、他の関係者が所定人数以上認めれば、ビジター等に対してそれら関係者と同等のセキュリティレベルを自動付与する。他の関係者たちの認証は、ビジターがそれら関係者たちと同行してリーダ・ライタの通信範囲内を通過するときに、自動的に行われるようにする。すなわち、例えばオフィス等に入るために、入り口のリーダ・ライタの近傍に、仮のＲＦＩＤを持った人と、その人の認証に要する所定人数の関係者とが来れば、リーダ・ライタでそれを検知して、仮のＲＦＩＤにそれら関係者と同等のセキュリティレベルの情報をリーダ・ライタから書き込むようにする。

【００７５】これは先に述べた実施形態４の場合と似ている。異なる点は他に所定人数居ればドアが開くのではなく、ドアを開けることのできる別のＲＦＩＤを作る（より厳密にはＲＦＩＤにドアを開けることができるセキュリティレベルを付与する）という点である。

【００７６】ただし、どんなカードでもそのセキュリティレベルがコピーできると、高いセキュリティレベルのカードをなんらかの方法で入手してそのレベルを自分のものにコピーできてしまう。このような不正使用を防止しようとするならば、例えば仮のＲＦＩＤカードに、仮のカードであることを示すセキュリティ上のプロパティ情報を持たせればよい。こうすることにより、セキュリティレベルのコピーは、限定された特殊な仮のカードだけにしかコピーできない。なお、仮のカード自体は、守衛所などで一定の手続を踏んで交付されるものなので、

かなりのレベルのセキュリティが確保されている。仮のカードの有効期限を例えば１日限りなどと限定しておけば、更にセキュリティが向上する。

【００７７】本実施形態の処理は次のようになる。すなわち、セキュリティ管理装置１０４が、あるリーダ・ライタから、同時に読み取った複数のＲＦＩＤのセキュリティ情報を取得した場合、その中に仮のＲＦＩＤのセキュリティ情報が含まれているかどうかを判定する。仮のＲＦＩＤかどうかは、前述した仮カードを示すプロパティ情報が含まれているかどうかで判定してもよいし、仮ＲＦＩＤに使うＩＤ番号を予め限定してそれを管理装置１０４に登録しておき、読み取ったＲＦＩＤ群の中にそれに該当するものがあるかどうかで判定してもよい。同時に読み取ったＲＦＩＤ群の中に、仮のＲＦＩＤがあれば、管理装置１０４は、同時に読み取った他のＲＦＩＤ群セキュリティレベルの値を、リーダ・ライタを介してその仮のＲＦＩＤに書き込む。

【００７８】一般に、ＲＦＩＤを忘れた者は、同部署の者に同行を求めれば、ほとんど自分自身のものと同等のセキュリティレベルを仮ＲＦＩＤにコピーできるので、その日の業務の支障が大幅に減る。

【００７９】本実施形態によれば、有効なＲＦＩＤを持つ者と同行するだけで、仮のＲＦＩＤにその者と同等のセキュリティレベルを自動書き込みできるので、仮カード発行場所で所望のセキュリティ設定を人手で行うなどの手間なしで、所望のセキュリティを実現できる仮のＲＦＩＤが得られる。

【００８０】［実施形態６］この実施形態は請求項１０に関する。実施形態１，２，３において、ユーザのセキュリティレベルが文書のセキュリティレベル未満の場合、複写がなされない。この場合、本実施形態では、セキュリティ管理装置１０４から複写機１０６に対して、複写許可条件が満たされないことを示すエラーコードを送る。このエラーコードを受け取った複写機１０６のコントローラは、それに基いて、複写機に設けられる操作パネルの液晶表示装置などに、そのコードに対応した例えば図１２に示すような複写不可のメッセージを表示する。可視的表示の代わりに、複写機１０６に音声発生装置を付け、音声でもってユーザに複写不可の旨を通知するようにしてもよい。

【００８１】この実施形態によれば、ユーザは、どのような理由で複写機を使えないかを知ることができ、知らないがゆえに起こる時間の無駄が省ける。

【図面の簡単な説明】

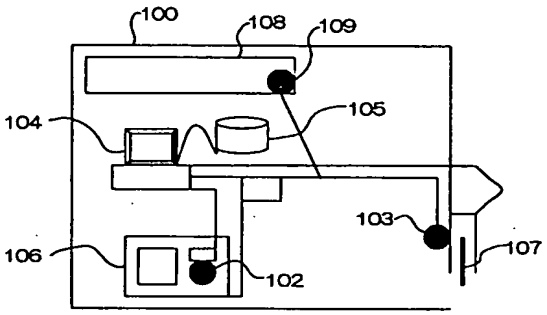
【図１】　本発明に係る複写管理を適用した機密室の構成を示す図である。

【図２】　ユーザ及び機密文書とそのＲＦＩＤを示す図である。

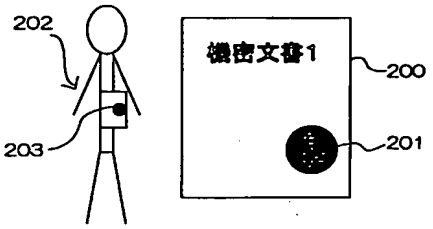
【図３】　リーダ・ライタを装着した複写機の概略を示す図である。

【図４】　ＲＦＩＤが持つセキュリティ情報のデータ構造の一例を示す図である。
【図５】　セキュリティ管理装置による複写機のセキュリティ制御の手順を示すフローチャートである。
【図６】　複写動作の許可条件のテーブルの例を示す図である。
【図７】　実施形態２のリーダ・ライタのアンテナ配置の一例を示す図である。
【図８】　実施形態３のリーダ・ライタのアンテナ配置の一例を示す図である。
【図９】　実施形態４のシステムの全体的な処理手順を示すフローチャートである。
【図１０】　実施形態４のシステムで、ＲＦＩＤが１つしか検出できなかった場合の処理を示すフローチャートである。
【図１１】　実施形態４のシステムで、ＲＦＩＤが２以上検出できた場合の処理を示すフローチャートである。
【図１２】　実施形態６における複写不可の表示の例を示す図である。
【符号の説明】
１００　機密室、１０２，１０３，１０９　リーダ・ライタ、１０４　セキュリティ管理装置、１０５　記憶装置、１０６　複写機、１０７　ドア、１０８書棚、２０１，２０３　ＲＦＩＤ、３００　複写機、３０１　複写面、３０２カバー、３０３　リーダ・ライタ。

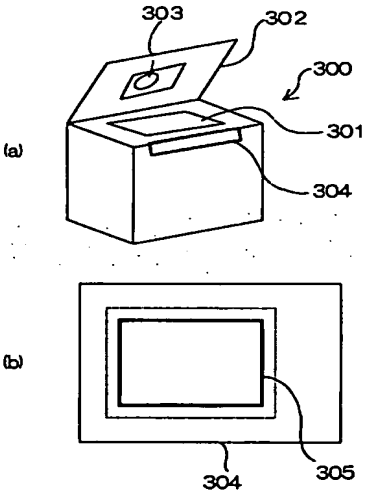
【図１】



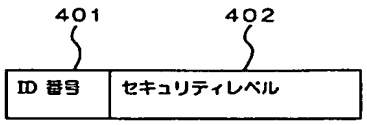
【図２】



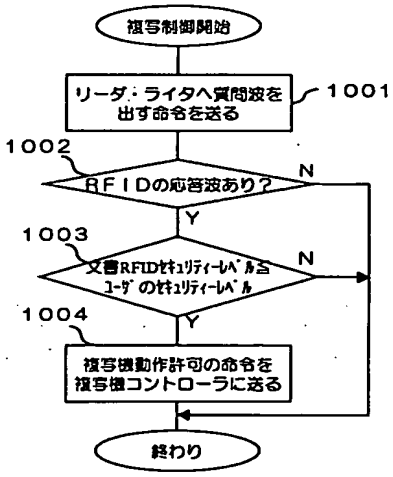
【図３】



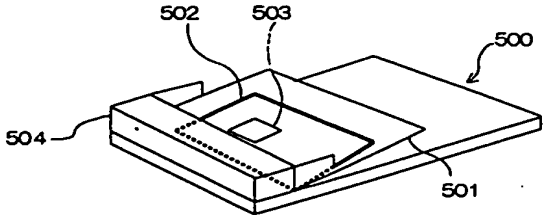
【図４】



【図５】



【図７】



【図６】

(a)

文書ID	許可ユーザID
D1	U1, U2, ...
D2	U1, U4, ...
...	...

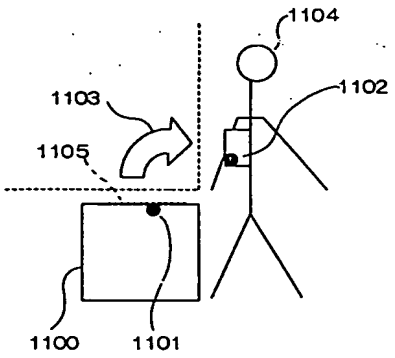
(b)

文書 セキュリティレベル	許可ユーザID
レベル1	U1, U2, ...
レベル2	U2, U4, ...
...	...

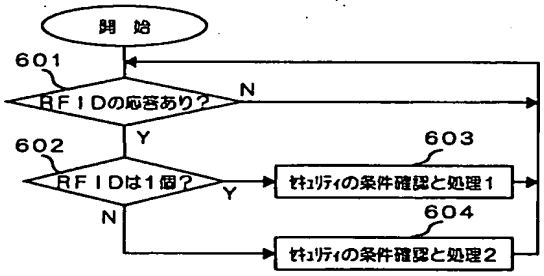
(c)

文書ID	許可ユーザ セキュリティレベル
D1	レベル1以上
D2	レベル3以上
...	...

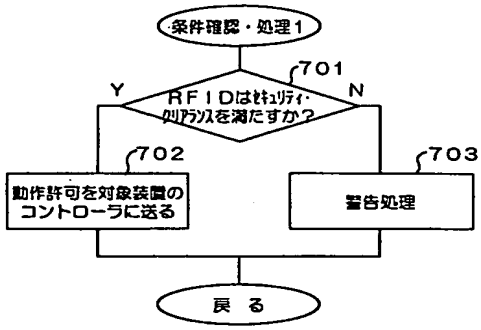
【図８】



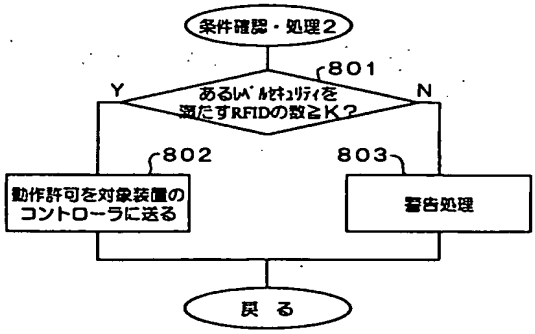
【図９】



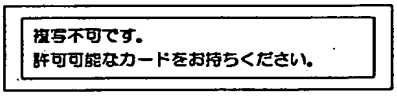
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０６Ｋ	19/07		Ｈ０４Ｂ	5/02		５Ｊ０４７
	19/10		Ｇ０３Ｇ	21/00	３９０	５Ｊ１０４
Ｈ０１Ｑ	1/12				５５４	５Ｋ０１２
Ｈ０４Ｂ	5/02		Ｇ０６Ｋ	19/00	Ｈ	９Ａ００１
Ｈ０４Ｌ	9/32				Ｒ	
			Ｈ０４Ｌ	9/00	６７３Ａ	
					６７３Ｅ	

Ｆターム(参考) 2H027 EJ02 EJ04 GA23 GA30
2H034 BF08 FA01
5B017 AA05 AA06 BA05 BA06 BB03
BB06 CA16
5B035 AA14 BB09 BC00 CA23
5B058 CA15 KA31 YA13
5J047 AA07 AA08 AA09 AA17 AA19
BG06 EF05
5J104 AA07 KA01 NA05 NA35 NA36
NA41 NA42 PA14
5K012 AA03 AB03 AB04 AC06 BA02
BA07
9A001 CC05 HH34 JZ35 LL03